



UNITED STATES DISTRICT COURT

for the
Eastern District of Virginia

In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)

IN THE MATTER OF THE SEARCH OF
ELECTRONIC DEVICES COLLECTED AS EVIDENCE
LOCATED AT 1970 E. PARHAM ROAD, RICHMOND, VIRGINIA
23228

Case No. 3:20sw342

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

At 1970 E. Parham Road, Richmond, Virginia 23228, are the devices set forth in Affidavit Attachment A.

located in the Eastern District of Virginia, there is now concealed (identify the person or describe the property to be seized):

At 1970 E. Parham Road, Richmond, Virginia 23228, are the devices set forth in Attachment A containing the evidence set forth in Affidavit Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section
 17 U.S.C. Section 506(a)(1)(B) & Copyright Infringement
 18 U.S.C. Section 2319(c)

Offense Description

The application is based on these facts:

See Attached Affidavit

- ☒ Continued on the attached sheet.
☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Reviewed by AUSA/SAUSA

Michael C. Moore

Printed name and title


 Applicant's signature

Clifford P. Greene, Special Agent, FBI

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by
 Telephone _____ (specify reliable electronic means).

Date: November 12, 2020

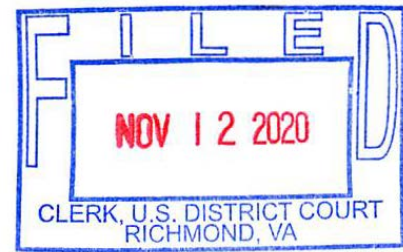
City and state: Richmond, Va.

/s/

Judge's signature

Elizabeth W. Hanes, U.S. Magistrate Judge

Printed name and title



IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Richmond Division

IN THE MATTER OF THE SEARCH OF
ELECTRONICS BELONGING TO HAIZHOU
HU, COLLECTED AS EVIDENCE,
LOCATED AT 1970 E. PARHAM ROAD,
RICHMOND, VIRGINIA 23228

Case No. 3:20sw342

AFFIDAVIT IN SUPPORT OF AN
APPLICATION UNDER RULE 41 FOR A
WARRANT TO SEARCH AND SEIZE

I, Clifford P. Greene, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the Federal Bureau of Investigation (FBI) and have been since June 2012. I am currently assigned to the Richmond Division of the FBI. I received formal training at the FBI Academy in Quantico, Virginia, on federal criminal statutes and rules, and conducting criminal and national security investigations, including the writing and executing of search and arrest warrants. My principal duties include the investigation of various criminal violations, to include espionage, economic espionage, and theft of intellectual property and trade secrets.

2. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—multiple electronic devices—more fully described in Attachment A, which are currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

3. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that information associated with the collected electronic devices constitutes evidence, fruits, and instrumentalities of the following offenses: copyright infringement, in violation of 17 U.S.C. § 506(a)(1)(B) and 18 U.S.C. § 2319(c).

4. The facts in this affidavit are based on my personal observations, my training and experience. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all my knowledge about this matter.

IDENTIFICATION OF THE DEVICES TO BE EXAMINED

5. The property to be searched are as follows: a silver Meizu cell phone, a silver iPhone, a Lenovo (IBM) ThinkPad laptop, a WD Elements hard drive, a Toshiba hard drive, a light blue thumb drive and an iPad with blue case (collectively, the “DEVICES,” as described more fully in Attachment A). The DEVICES are currently located at the FBI’s Richmond Field Office, 1970 E. Parham Road, Richmond, Virginia 23228.

6. On September 17, 2020, this Court previously approved a warrant to search the DEVICES identified above. However, based on more recently-obtained information, described in detail below, after the forensic imaging of some of the DEVICES, this updated affidavit is being submitted in support of a new application for a search warrant authorizing the examination of the DEVICES and previously created forensic images pursuant to Rule 41 of the Federal Rules of Criminal Procedure.

BACKGROUND

7. On August 25, 2020, U.S. Customs and Border Protection (CBP) agents assigned to Chicago's O'Hare International Airport were conducting routine screening of outbound travelers in the boarding process for China Eastern flight number MU 7226 to Qingdao, China. One of those travelers was an individual by the name of HAIZHOU HU.¹ When CBP questioned HU regarding the nature of his activities in the United States, HU provided conflicting and incriminating statements regarding his activities while conducting U.S.-government funded research at the University of Virginia (UVA) Department of Mechanical and Aerospace Engineering (MAE) under the guidance of an individual, referred to in this affidavit as "Professor 1." A forensic review of HU's electronic DEVICES revealed UVA-research related files stored on HU's laptop, to include bio-inspired research simulation software code subject to copyright protection developed by Professor 1. Professor 1 has been developing this code over the last 17 years and taken steps to derive value from the code by safeguarding it.²

¹ From record checks, HU entered the United States on a J1 Visa on March 30, 2019. HU's visa was issued on March 15, 2019 with an expiration date of March 1, 2020; however, due to the COVID-19 outbreak, HU was unable to travel home and his visa was extended. On August 25, 2020, HU was encountered by CBP attempting leave the U.S. on a flight from Chicago. After HU's arrest, UVA terminated HU's J1 visa status effective August 31, 2020 due to the ongoing investigation into theft of proprietary information from UVA.

² Copyright law protects all "original works of authorship fixed in any tangible medium of expression, now known or later developed, from which they can be perceived, reproduced, or otherwise communicated, either directly or with the aid of a machine or device." 17 U.S.C. § 102(a). It includes "literary works," which includes works "expressed in words, numbers, or other verbal or numerical symbols or indicia." 17 U.S.C § 101. A work is protected by copyright law from the moment it is created, even if it is not registered. 17 U.S.C. §§ 101-102(a), 408(a).

PROBABLE CAUSE

8. During the interview with CBP, HU said he was conducting research at UVA on bio-mimics and fluid dynamics which could be used for underwater robotics. HU knew that this research was funded by the United States government in the form of a grant by the U.S. National Science Foundation (NSF), which is an independent federal agency created by Congress to promote the progress of science, advance the national health, and secure the national defense. HU stated Professor 1 runs the Flow Simulation Research Group (FSRG) that is a multi-university collaborative funded by the Office of Naval Research.³ HU approached Professor 1 to ask about conducting research at UVA after Professor 1 had given a lecture on bio-mimics in aerodynamics at Beihang University in 2017. Beihang University is located in the People's Republic of China (PRC). HU stated the costs associated with his research in the United States were paid for by a scholarship from the Chinese Scholarship Council (CSC).

9. HU said that he works for the Chinese Key Laboratory for Fluid Dynamics located at Beihang University.⁴ HU stated that the Chinese-equivalent of the NSF funds this Key Laboratory, and it also receives funding from the Chinese Air Force. According to the Curriculum

³ The Office of Naval Research (ONR) coordinates, executes, and promotes the science and technology programs of the United States Navy and Marine Corps through schools, universities, government laboratories, and non-profit and for-profit organizations. It provides technical advice to the Chief of Naval Operations and the Secretary of the Navy and works with industry to improve technology manufacturing processes. The ONR mission is to foster, plan, facilitate and transition scientific research in recognition of its paramount importance to enable future naval power and the preservation of national security.

⁴ Per the Australian Strategic Policy Institute, Beihang University contains a high number of defense laboratories and defense research areas. One of the major defense laboratories listed is the National Laboratory for Computational Fluid Dynamics.

Vitae submitted with his U.S. visa application, HU had previously attended a Chinese university named Harbin University.⁵ Hu told CBP agents that at Harbin University, he worked in the Key Laboratory for Underwater Robot Technology. When asked how that laboratory was funded, at first, HU said he was not sure. HU was then asked if the laboratory was funded by the People's Liberation Army ("PLA"), which is the armed forces of the PRC, to which HU replied, "Of course." HU stated that, as part of his scholarship, he was directed by the Chinese Scholarship Council to upload summary reports regarding his UVA research every 6 months.

10. HU was asked if his electronic devices stored any of the research that he conducted at UVA. HU stated he had all his research. At first, HU indicated that Professor 1 knew he was taking his research with him. Later, HU stated that neither Professor 1 nor anyone else was aware he was taking his research back to China.⁶

11. A basic media exam of HU's devices was conducted and HU's devices were detained. During the interview, HU admitted he had coding files on his computer that Professor 1

⁵ Per the Australian Strategic Policy Institute, Harbin Engineering University (HEU) contains multiple PRC national defense key laboratories. One key laboratory of note is the National Defense Key Laboratory of Underwater Vehicles Technology also known as the "Military-use Underwater Intelligent Robot Technology National Defense Science and Technology Key Laboratory." Under an agreement in 2007 between HEU and the PLA Navy, the PLA Navy committed to developing HEU's capacity as a platform for R&D in military technology and for training defense personnel.

⁶ On or about October 16, 2020, UVA IT representatives discovered that in June 2020, there had been a significant spike in the Internet connectivity from the desktop assigned to HU. UVA IT representatives further discovered that approximately 1 TB of data had been transmitted around that time from HU's computer to an Internet Protocol address resolving to China, which the FBI is further investigating.

would not want him to have. Subsequent review of HU's laptop identified approximately 9,600 F90 FORTRAN source code files used for bio-inspired learning, research, and modeling.

12. On August 26 and 27, 2020, agents of the FBI and Customs and Border Patrol interviewed Professor 1, who is a Professor at the UVA MAE. Professor 1 knew HU and confirmed that HU had been a researcher in Professor 1's laboratory from approximately March 2019 to August 2020.

13. Professor 1 stated the F90 source code files were used during simulations conducted in furtherance of bio-inspired fluid mechanics research funded by NSF. Professor 1 categorized the file types utilized in his research simulations into four categories: 1) pre-processing code 2) executable files; 3) post-processing data; and 4) "core code." According to Professor 1, researchers – including HU – who were conducting simulations in Professor 1's laboratory at UVA had access to the first three types (i.e., pre-processing code, executable files and post-processing data). However, as to the "core code," according to Professor 1, the access was strictly guarded.⁷ According to Professor 1, these strict limitations were by design because the core code was proprietary, and he had been developing it over the last 17 years. Professor 1 further described the core code as the preeminent bio-inspired research simulation software in the world. Other

⁷ Professor 1 acknowledged that he placed additional restrictions on access to newer versions of the core code. For instance, Professor 1 advised that third year students in his lab were only granted access to the 2014 version of the core code, communicating to those students the expectation they would protect it by not providing it to anyone else without his permission, and by keeping it housed in a locked folder. By contrast, Professor 1 stated in a subsequent September 2020 interview described below that only two graduate students have access to the 2019 version and only one of them has access to the 2020 version, reflecting greater efforts to protect the core code in its newest state.

universities and commercial vendors have requested access to the core code for both research and commercial uses. However, Professor 1 has not shared it because he wishes to maintain his unique competitive advantage in conducting research in the bio-inspired fluid mechanics field.

14. As described above, Professor 1's unique core code was written and updated by Professor 1 and selected research assistants over the course of 17 years. Therefore, it is a work of authorship independently created by the authors (e.g., not copied from another previous work). *See* 17 U.S.C. § 102(a) (copyright law protects all "original works of authorship fixed in any tangible medium of expression").

15. Because of the importance and value of the core code, Professor 1 stated to the FBI in August 2020 that only three people have access to the core code: Professor 1 and two graduate students who work under Professor 1 on the continued development of the core code. Professor 1's ability to conduct simulations using this core code resulted in his receiving numerous grants as a researcher, including but not limited to two current NSF grants totaling \$1.8 million dollars. According to a UVA Applied Research Institute official, a U.S.-based company, Company One, has developed similar simulation software; open source reporting indicates Company One's revenue in 2019 exceeded \$1.5 billion dollars. While the core code is not for sale through normal retail channels, your affiant believes, based on the foregoing, as well as his training and experience, that the core code would have a retail value of more than \$1,000.

16. The core code is stored on a UVA high performance computer cluster "Cayley" (Cluster A) in UVA's data center. Some researchers in Professor 1's laboratory may access Cluster A through UVA's Virtual Private Network (VPN). UVA's VPN contains language that advises all individuals using the network:

You are now connected to the University of Virginia network, which is available for authorized use only. All traffic and actions are subject to University's policies (<http://uvapolicy.virginia.edu/>). By connecting to the university's network, you acknowledge and consent to these terms.

17. Because the “core code” was stored on tangible computers, it was recorded in some tangible medium by the authors. *See* 17 U.S.C. § 102(a) (copyright law protects all “original works of authorship fixed in any tangible medium of expression”).

18. UVA's policy entitled, “IRM-002: Acceptable Use of the University's Information Technology Resources,” states, among other things, that users must not:

- Obtain or attempt to obtain unauthorized access to the University's IT resources; [and]
- Circumvent or attempt to circumvent security controls on the University's IT resources [.]

19. For every researcher who has access to Cluster A, their access is individually reviewed and approved by Professor 1 and administered by UVA's Information Technology personnel. Each researcher's profile determines what information on Cluster A they are able to access. Each individual researcher has a “home” storage space that only that individual can access, and each individual may also access a “shared” storage space which is shared among other users. Professor 1 believed that he stored his core code on the home storage space for himself and the two graduate students with whom he works closely on the core code, and that the core code was not generally available on the “shared” storage space. Access to each researcher's profile on Cluster A is controlled by entering a unique username and password.

20. In or about July 2019, HU asked Professor 1 for access to Cluster A, the high-performance computer cluster on which the code resides. Professor 1 granted HU access to Cluster

A's shared storage space, but prior to granting HU access, Professor 1 directed a research assistant 1 (hereinafter "Research Assistant 1") to search the shared space for any unprotected core code files. Research Assistant 1 located one of the core code files in the shared space and advised Professor 1 of his finding. Professor 1 contacted UVA Information Technology personnel to remove the file located in the shared space. UVA Information Technology personnel contacted Professor 1 when the removal was complete. Professor 1 stated HU requested access to the core code from both of the UVA graduate students within his lab with access, but both denied HU's request.

21. On August 27, 2020, Professor 1 and FBI agents reviewed the F90 code files that were located on HU's laptop computer as he sought to leave the United States. Using a keyword search, Professor 1 and agents identified approximately 55 of his core code files. Professor 1 indicated the files constituted the entirety of his core code he had been developing over the last 17 years. Professor 1 was extremely concerned that if his core code was taken for use outside his research lab, it would compromise his competitive advantage in the research field and could be exploited for various commercial, governmental and military applications by other entities, including universities, companies, or countries.

22. On August 27, 2020, during a custodial interview with FBI Agents, HU advised that Professor 1 did not give him permission to take any of his work back to China, and that he downloaded the F90 files from a folder called "clean picar."⁸ HU advised that Professor 1 would

⁸ The core code was in the F90 files HU downloaded, and through previous interviews the word "picar" was another term used to describe the F90 files.

be upset if he learned that HU had downloaded the F90 files and that HU had them in his possession.

23. HU described how he downloaded the F90 files onto a laptop and opened them in Microsoft Visual Studio to look at them, noting he had hundreds to thousands of files. HU confirmed that coding was not his area of expertise and in his lab back in China they lacked the ability to create this type of code to conduct research.

24. On September 18, 2020, FBI agents interviewed Professor 1 during which he reiterated that the core code had controlled access. Professor 1 considered the make-up of his student base as two groups: the “inner circle,” and the visiting scholars. The students of the “inner circle” gradually got access to the core code because they were with him for four to five years. The visiting students were not allowed access to any of the core code because they were only with his lab for six months to a year, returning home once their research was complete. Instead the visiting scholars were granted access only to the pre-processing code, executable files and post-processing data.

25. Professor 1 recounted a conversation directly with HU advising HU that he would not get access to the core code during his time at UVA and not to ask for it. Professor 1 advised that even though he clarified to HU that HU would not get access to the core code, HU repeatedly asked for it from Professor 1 and other students in Professor 1’s lab. By way of interview, all students in Professor 1’s lab denied giving HU access to the core code. On no occasion did Professor 1, or anyone else, tell HU he was permitted to copy the core code.

26. Professor 1 described that the students of the “inner circle” get access gradually, whether it was a limited number of files of the core code or access to previous versions. He went

on to describe how some “inner circle” students had access to the 2014 version of the core code to conduct research. Professor 1 stated that only Authorized Students 1 and 2 had access to the 2019 version of the core code and only one of them had access to the 2020 version as they were helping to continue development of the core code. Professor 1 advised that he had a backup of the core code on discs that were in his office.⁹ During that September 18, 2020 interview the FBI learned that a former graduate student who was granted access to a version of the core code had saved it to an external hard drive and left it on his work station in the lab.

27. During the same interview with Professor 1, a search was conducted on Cluster A within the shared space to confirm that none of the core code was available to users of the shared space. The results of the search showed that Professor 1’s core code was available in various folders on Cluster A’s shared space, and those folders could be accessed by using HU’s assigned user profile.

⁹ On October 9, 2020, in a follow up discussion, Professor 1 noted that the backups of the core code were in his office in a box on a bookshelf. Professor 1 stated that his office was always locked and only accessible by himself or the school janitor.

Professor 1, who currently works remotely due to the pandemic, estimates there were anywhere from 5-8 backups located in his office and they were labeled with the date of the backup which would help identify the version of the core code. A backup was completed when space was needed and/or when students were leaving his program that would have been assisting with the core code. The backups in his office from 2012-2014, 2016 and 2018-2019, were not encrypted because he did not know how to do this. Professor 1 has his two offices on campus. One office is in the MAE where his main lab is, and another office is within a 5-minute walk. Since September 18, 2020, all backups have been moved to the secondary office and are locked in a cabinet to which only he has the key. That office location is always also locked.

28. Professor 1 confirmed the search returns showed that students in his lab had numerous files of core code on shared space that he was previously unaware of and did not expect to find. UVA Information Technology personnel were able to verify that the user profiles and folder locations where the core code was stored were unlocked and accessible if/when HU was to access Cluster A.

29. Contrary to Professor 1's belief that access to the core code had been strictly guarded per his request, both through his policies and enforcement of those policies (such as admonishing Hu that Hu could not access the core code when HU repeatedly asked for a code HU believed he was unable to access), for reasons unknown the core code was accessible by students in his lab on the shared space of Cluster A. Professor 1 never gave permission for HU to reproduce that core code.

30. HU informed the FBI that after acquiring the core code, he had reviewed the files in his possession. HU acknowledged to the FBI that Professor 1 did not give him permission to take any of his research back to China, nor did HU inform Professor 1 that he had downloaded the core code knowing Professor 1 would be upset if he knew HU had them.

31. Based on the above facts, and my training and experience, I believe that HU willfully infringed the rights of Professor 1, UVA, and/or NSF to reproduce the copyrighted work (i.e., the core code). *See* 17 U.S.C. § 106(1) ("the owner of copyright under this title has the exclusive rights to ... reproduce the copyrighted work in copies"; 17 U.S.C. § 506(a)(1)(B).

32. The electronic devices are currently in the lawful possession of the FBI. The FBI took custody of the electronic devices from CBP on August 27, 2020, the day of HU's arrest.

33. The FBI sought and obtained a search warrant on September 17, 2020, prior to the September 18, 2020, interview described above, based on an affidavit with facts that supported probable cause for computer intrusion and theft of trade secrets in violation of federal law. In part, only two of the seven devices for which the warrant was sought were imaged by the FBI, and no further search was conducted. Based on new information received on September 18, 2020, including that the core code was in a shared space on Cluster A, the FBI declined to continue with the current search warrant and moved to amend and acquire a new warrant in support of executing the search of HU's electronic devices. I seek this warrant out of an abundance of caution to be certain that an examination of the electronic devices will comply with the Fourth Amendment and other applicable laws.¹⁰

34. The electronic devices are currently in storage at the FBI's Richmond Field Office, 1970 E. Parham Road, Richmond, Virginia 23228. In my training and experience, I know that the electronic devices have been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the electronic devices first came into the possession of the FBI.

TECHNICAL TERMS

35. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. **Internet:** The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections

¹⁰ The previous warrant asserted probable cause to believe that information associated with the collected electronic devices constitutes evidence, fruits, and instrumentalities of the following offenses: unauthorized use of a computer, in violation of 18 U.S.C. § 1030, and theft of trade secrets, in violation of 18 U.S.C. § 1832.

between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

- b. **Internet Protocol address (or simply “IP address)** is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.
- c. **Log Files** are records automatically produced by computer programs to document electronic events that occur on computers. Computer programs can record a wide range of events including remote access, file transfers, logon/logoff times, and system errors. Logs are often named based on the types of information they contain. For example, web logs contain specific information about when a website was accessed by remote computers; access logs list specific information about when a computer was accessed from a remote location; and file transfer logs list detailed information concerning files that are remotely transferred.
- d. **Storage Medium** is any physical object upon which computer data can be recorded. Examples include (but not limited to) hard disks, thumb drive, external hard drive, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media. Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.
- e. **Wireless Telephone:** A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.
- f. **Tablet:** A tablet is a mobile computer, typically larger than a phone yet smaller than a notebook, that is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to access the Internet through cellular networks, 802.11 “wi-fi” networks, or otherwise. Tablets typically contain programs called apps, which, like programs on a personal computer, perform

different functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks.

36. Based on my training, experience, and research, I know that electronic devices have capabilities that allow them to serve as a wireless telephones, digital cameras, portable media player, GPS, personal digital assistant, access the internet, mass storage devices of information as well as the ability to communicate in an encrypted environment void of detection from outside persons to include law enforcement, among other uses. In my training and experience, examining data stored on electronic devices of this type one can uncover, among other things, evidence that reveals or suggests who possessed or used the device, information stored on the device, information downloaded, encrypted communications, contacts and many other items.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

37. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

38. **Forensic Evidence:** As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
 - c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
 - d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
 - e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.
39. **Nature of Examination:** Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.
40. **Manner of Execution:** Because this warrant seeks only permission to examine devices already in law enforcement’s possession, the execution of this warrant does not involve the

physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

41. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the electronic devices described in Attachment A to seek the items described in Attachment B.

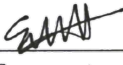
OATH

The information in this affidavit is true to the best of my knowledge and belief.

Respectfully submitted,

s/Clifford P. Greene
Clifford P. Greene, Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on November 10, 2020.

/s/ 
Elizabeth W. Hanes
United States Magistrate Judge

ATTACHMENT A

The property to be searched are as follow: a silver, Meizu cellular phone, with no visible serial number, a silver, iPhone Model A1660, with no visible serial number, a Lenovo IBM ThinkPad, Serial Number: PF-1J5XKC, a WD Elements, Serial Number: WXE2E100LUS6, Part Number: WDBU6Y0020BBK – EB external hard drive, a Toshiba, Serial Number: 16O3T8PYTTT4, Part Number: HDTB310YK3AA external hard drive, a USB thumb drive, light blue, label “12”, no visible serial number, and an iPad with blue case, no visible serial number. The electronic devices are currently located at 1970 E. Parham Road, Richmond, Virginia 23228.

ATTACHMENT B

1. All records on the Devices described in Attachment A that relate to violations of Title 17, United States Code, Section 506(a)(1)(B), and Title 18, United States Code, Section 2319(b)(3), and involve HAIZHOU HU including:

- a. any conversations, whether through text messages or other applications, concerning the theft of or reproduction of materials subject to copyright;
- b. any information relating to (including names, addresses, phone numbers, or any other identifying information) or communications with HU and possible co-conspirators or associates concerning the theft or reproduction of copyrighted material;
- c. any information relating to the research HU conducted, to include research that he may be in possession of that he was not authorized to have access to while at UVA;
- d. any information relating to the copyright protected F90 code that HU may be in possession of to include communications, downloads, transfers, reproductions, uses, etc.
- e. any information relating to HU's motive to reproduce copyright protected material, including research HU conducted at Beihang University and/or Harbin Engineering University, and HU's affiliations with the PRC military or any other PRC entity;
- f. Records of HU's UVA profile use history to include IP logs, proxy services, designed to hide the IP address of the server or of the user.

2. Evidence of user attribution showing who used or owned the electronic devices at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

As used above, the terms “records” and “information” includes all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.